Enclosed
Purple Tree Technologies Responses to
FCC CMSAAC “request for comments” for PSHSB Docket No. 07-287

Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of

The Commercial Mobile Alert System

PS Docket No.07-287

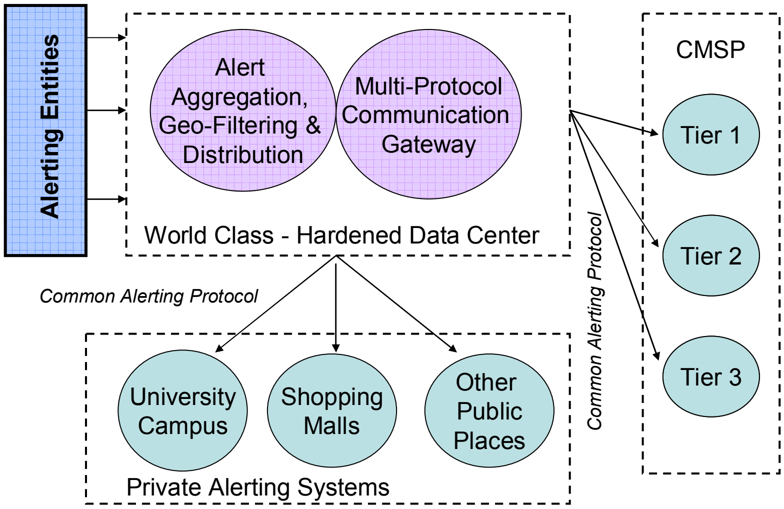
Background:

Purple Tree Technologies (PTT) and their partner Electronic Data Systems (EDS) since 2004 have conducted substantial research and development specifically in the areas of Emergency Alert Aggregation and Transmission. This research and development have resulted in the creation of an end-to-end Emergency Alert Response System that functions over cellular and private communication systems. Our research and development efforts revolve around:

- processing CAP and non-CAP alerts from emergency alerting agencies,
- geographically targeting alert transmission based on message content, and
- transmission and reception of the CAP formatted alert messages to cellular and non-cellular end point devices.

Our findings are the most current findings available in the industry. Our comments below are shared to aid the commission and the industry in their decision making process in the coming months.

FCC statement: *Section 602(a) of the WARN Act requires that the Commission adopt technical standards, protocols, procedures, and other technical requirements based on the recommendations of the CMSAAC that will enable commercial mobile service alerting capability for CMS providers that voluntarily elect to transmit emergency alerts. The CMSAAC has recently completed its report,*[21] *and we seek comment generally on all the recommendations contained therein. Accordingly, we seek comment on the technical standards, protocols, procedures and other requirements that should be adopted to facilitate the transmission of emergency alerts by CMS providers.*[22] *We ask whether these recommendations, if adopted, would satisfy the requirements of the WARN Act and our goal of ensuring a robust, reliable and effective CMAS that could, in conjunction with other alerting systems and technologies, be used to transmit emergency alerts to all Americans, including those with special needs and those who do not speak English. We seek comment on whether the CMSAAC recommendations* *present an effective mechanism for alert originators at all levels of government to initiate emergency alerts and whether these recommendations could be implemented using a myriad of current and future technologies. Commenters should review all of the recommendations and comment, where appropriate, on the manner in which each of the recommendations contributes to an effective, unified system for the delivery of alerts over commercial mobile systems as envisioned by the WARN Act.*[23] *We further seek comment on any alternatives to the CMSAAC's recommendations. Comments that suggest alternatives to the CMSAAC's recommendations should address with sufficient detail how their proposed alternative would promote an effective CMAS as envisioned by the WARN Act*



PTT Responses: The CMSAAC have provided the Commission a solid first draft of an alerting system. However, the recommendations of the CMSAAC do not adequately meet the Commission's requirements for timely and accurate information as well as distributing alerts over diverse communications platforms. The Commission lists the Virginia Tech shootings as the need to meet these requirements. Our work over the last year in developing the technologies and systems to provide geo-targeted emergency alerts and from meeting with organizations on their alerting needs in light of the Virginia Tech and Omaha mall shootings have brought us the realization that the community requires an alerting system that is geo-specific, to a geographic area smaller than a county. In addition the system should be flexible and accessible by first responders. The CMSAAC's recommendations are only adequate for large scale events, weather, natural disasters, and national emergencies. It is not adequate to meet the current alerting needs of events like the Virginia Tech or Omaha mall shootings.

The PTT work on these issues in 2007 has led us to design a multi-tiered system that interacts with Tier 1, 2, & 3 CMSP's (see figure) as well as emerging private systems (e.g. university campus and shopping malls). It is an end-to-end system that accommodates the CMSAAC's recommendations and serves to provide alerts for large scale events, small local events, is usable by the first responders and targets alerts to a very specific geographic area, even a specific display and a shopping mall.   We believe that ultimately the Alert Aggregation function should have event processing to direct alerts intelligently. The function of filtering alerts may be relatively simple for a Tier 1 carrier, but lower Tier CMSP's, universities, schools, shopping malls, industrial facilities, city areas and other implementations should only be sent alerts that affect their service territory. Furthermore, the connectivity between these tiers should be standardized and open to allow interoperability between different solution providers.

Through our research and development, we know the capability is present to send alerts at a granularity much finer that that of a county. We also know that Alert Aggregator and Alert Gateway can send alerts to CMSPs that impact only the area that they cover. We provide the

Commission more details on the results of our work in a section of recommendations/alternatives at the end of this document.

We are generally in agreement with the requirements and recommendations from the CMSAAC. We do have some comments in the following areas, though:

a. The scenarios for multiple alerts (4.5.1 and 4.6) do not really address whether/how the system would detect duplicate alerts being issued by two different agencies (e.g. an Amber Alert received from both NWS and the State authorities). These could appear on the surface to be different alerts, but might in fact be the same alert. We do not want users to receive multiple copies of essentially the same alert.

b. Section 7.4 acknowledges that the proposed recommendations could cause a 40% additional battery drain with current technology. However, the proposed solution seems to be dependent on hypothetical improvements in mobile hardware and infrastructure. Purple Tree Technologies' "wake-up signal" technology concept, based on listening for the local EAS activation signal, would be a useful innovation to prolong battery life.

c. In recommendations 10.3.2.11 and 10.3.2.29, it is unclear to what standard CAP messages that are not "formatted correctly" should be rejected. In our tests, many of the NOAA CAP messages fail to meet the OASIS CAP formatting guidelines in one way or another. In addition, it is unclear how the Alert Gateway will "inform" the Alert Originator of invalid message content.

d. We have some concerns about recommendation 10.4, in which the CMSAAC is essentially defining a new XML schema to define messages to be issued by the CMSPs. The PTT solution relies on the de facto standard Parlay X specification for Message Broadcast, which is neutral as far as "alert" information (because it can be used for many types of messages). What the committee proposes seems to be a non-standard hybrid of CAP and Parlay X. We are concerned that creation of an entirely new schema might complicate matters, particularly for small market carriers who are looking for simpler specifications and/or off-the-shelf solutions.

7. No question or comment is presented that requires a response.

8. **FCC statement**: *We seek comment on the availability of technologies now and in the future for the transmission of alerts over the CMAS. For example, to what extent do point-to-point and point-to multipoint technologies provide viable solutions for a national CMAS? In this regard, we note that, the CMSAAC raised concerns regarding the viability of point-to-point solutions for a national alerting system. We seek comment on these concerns. Specifically, can current generation point-to-point services such as short message service (SMS) be used to efficiently alert large populations of people within a short time frame? What impact would wireless 3G networks have on the SMS model?*

PTT Response: We agree that point-to-point technologies are not viable for emergency alerting purposes when a large number of subscribers in the same area need to receive an alert message on a timely basis. Any point-to-point solution whether or not it is subscription based will face significant challenges to deliver the alert in a timely fashion when considering the delivery priority schemas for SMS messages and the competing voice traffic inherent to emergency situations. Addressing alerts an individual "receiver" level will add significant burden to cell infrastructure.

9. **FCC Statement**: *Can point-to-multipoint technologies such as cell broadcast provide a viable transport solution for alerts transmitted over the CMAS? If current cell broadcasting does not provide a viable solution, what further development would be necessary to use cell broadcasting for the CMAS? Are there significant differences in how CDMA or GSM systems could employ cell broadcasting today and in the future? Are current mobile devices capable of receiving cell broadcast alerts?*

PTT Response: We believe that cell broadcast (CBS) is the right technology for sending CMAS alerts to a large number of subscribers in the same area on a timely basis. The only effective and viable, solution for transmitting an alert to a large audience is a broadcast technology like cell broadcast. Recent attempts to provide alerting using the current point-to-point SMS capability have failed to deliver messages in a timely manner. At Virginia Tech, for example, tests of the recently implemented SMS/Internet reliant solution required an average of 18 minutes to complete message delivery with a significant number of recipients that reported no message delivery at all[1]. The failure of the point-to-point SMS is the queuing necessary to send a message to each individual phone. This requires that the paging slots, and potentially traffic channels be used to deliver the high volume of messages. This places a large load on the system. This loading effect has caused the telecom companies and equipment manufactures to limit the number of SMS messages. In contrast a single broadcast will use a single paging slot and be received by a majority of the cell phones connected to a switch and do so with only minimal loading on the system. CBS overcomes capacity and priority issues within the cell infrastructure that will be under even more strain during an emergency or crisis situation.

The current CDMA air interface specification, IS-637, and the IS-824 extension to the IS-41 standards, include the specifications necessary for the implementation of broadcast SMS. However, no CDMA handsets in the North American market include these features, and we know of no telecom equipment manufactures that has enabled, or certified, this functionality in their switches, base station controllers (BSC), or base transceiver stations (BTS). However , PTT have successfully transmitted and received a cell broadcast at the Alcatel-Lucent LiveNet facility using specialized handsets, verifying

[1] Source: https://secure.hosting.vt.edu/www.vtnews.vt.edu/story.php?relyear=2007&itemno=673

that it is possible to transmit a cell broadcast message over "existing" CDMA telecom infrastructure.

Cell broadcast is functioning in GSM networks outside of the American market in over 20 countries. There are a limited number of handsets in the American market with this feature enabled and the feature is available on some of the GSM switches in use in the American market. There does not appear to be significant issues between GSM and CDMA systems. The current established and industry-accepted broadcast protocols and standards (IS-41, IS-637 and IS-824) have provisions for cell broadcast. Current mobile devices have firmware capability to receive cell broadcasts, however there are limitations in current application software to handle the receipt of a cell broadcast.

In addition, other low cost devices that are dedicated to message broadcast reception should be considered within the scope of this committee. This also applies to other integrated technologies which may have this capability.

FCC Statement: *We also seek comment, particularly from the EAS community, on whether a broadcast distribution model similar to that used to distribute EAS is consistent with the WARN Act and the CMAS. Could radio data systems like the Radio Broadcast Data System (RBDS), which do not require significant service provider infrastructure, nonetheless meet our goals for efficient delivery of alerts over the CMAS? What about emerging wireless broadcast technologies such as MediaFLO and DVB-H? Comments should include a discussion concerning the broad range of devices intended to utilize the CMAS and potential impact on the subscriber service experience.*

PTT Response: We have successfully tested broadcasting alert messages via cell broadcast over a CDMA network to CBS-enabled mobile phones in the lab. The primary issue with cell broadcast, though, is that most U.S. phones are not enabled out of the factory. This is a key issue that needs to be addressed by the U.S. providers before a nationwide CMAS is feasible. In addition PTT has created other specialized or non-phone devices to address populations that are not mobile phone subscribers.

10. **FCC Statement**: *The CMAS as proposed by the CMSAAC likely will require a higher layer protocol that carries meta-data (administrative information) with the alert message, and can send authentication and authorization data to the alert's originator. We seek comment on whether this higher layer protocol is necessary for the CMAS. We also seek comment on how point-to-point, point-to-multi point and broadcast models could carry this information and provide the recommended authentication information. We further seek comment on any alternative methods for transmitting this data.*

    PTT Response: We agree that a higher layer protocol will be required for message authentication and reliability between the Alert Gateway and each CMSP Gateway. Each integration point in the system must authenticate and authorize the connecting system. In addition each message should be non-reputable. In the system that the

CMSAAC has put forth it will require that an additional protocol be put into place to provide this functionality. However, we believe that the protocols put forth by the CMSAAC are incorrect and insufficient to provide the reliability, security, and effectiveness that the Commission requires. We recommend changes to correct this deficiency at the end of this document.

Individual delivery models should not carry authentication and authorization information. Once the alert aggregator has authenticated and authorized an alert provider, and once a CMSP has authenticated and authorized an alert gateway the system should assume that the message is correct and valid. The CMSP's delivery of the message across reference points D and E should require no other validation of the alert provider, aggregator, or gateway

11. **FCC Statement:** *What should be the Federal Government's role, if any, in managing the CMAS? The CMSAAC recommended that a Federal Government entity fulfill the roles of "Alert Aggregator" (i.e , receive, accumulate and authenticate alerts originated by authorized alert initiators using the Common Alert Protocol (CAP))* [26] *and the "Alert Gateway" (i.e., formulate an alert based on key fields in the CAP alert sent by the alert initiator and transmit the alert to corresponding gateways operated by each CMS provider). We seek comment on these recommendations. Is it necessary and desirable for a Federal government entity to assume these roles? If so, what Federal government entity would be appropriate?*

    PTT Response: We are not convinced that the Federal Government should be the sole acquirer, maintainer, and operator of the CMAS Alert Aggregator and Gateway components. However, the Federal Government should definitely provide guidelines and oversight as to how the Alert Aggregator and Gateway are configured and operated, specifically detailing how alerts are enter the system, and how alerts get dispersed to the various CMSP's and private alerting systems. We envision a model like the public-private nature of Amber Alert program. The private sector is more than capable of fulfilling these roles. The private sector can more easily adapt to the changing markets and technology requirements (e.g. connecting to private university or mall systems). We suggest that a public - private community be established initially with government sponsorship. This private, quasi-government community, in concert with Federal Agencies, will jointly establish a governance model for operation and participation in this national alerting community. The primary function of this entity however, will be to create the CMAS and rapidly deploy the alerting infrastructure with government sponsorship and industry participation.

12. **FCC Statement**: *The CMSAAC also recommended that all alerts, whether national or local, would be funneled through this aggregator. Is a centralized system best positioned to accomplish the goals of the CMAS as envisioned by the WARN Act? Would this run the risk of creating a single point of failure? Further, we seek comment on the government alerting system capability to a) support the aggregation of alerts from emergency agencies down to county and municipal levels, b) distribute alerts to a diverse range of potential alerting systems, and c) interact and determine*

the status of such connected alerting systems. What is the role of state emergency agencies in such a scheme? Should the aggregator concept be expanded to include state and county emergency agencies, such as state and county emergency operations centers (EOCs)? Could this be done in a manner that could track a state's role in any EAS activation? What equipment or security issues might be involved in expanding the scope of the system? What criteria should be established for determining the appropriateness of connecting an agency? What responsibilities should be attendant on connected agencies?

PTT Response: Our opinion is that the CMSAAC's current recommendations establish the needed foundation to achieve the requirement of distributing alerts to a diverse range of alerting systems. However, through our research and development efforts, we believe that the current recommendations do not meet this goal. In our responses to the Committee's request for comment we hope to share what we have learned in our efforts to develop an alerting system.

We agree with the concept of centralizing issued alerts an Alert Aggregator. There should definitely be redundancy for failover in any component in the infrastructure. We recommend to the commission that all <u>national</u>, and <u>state</u> alerts be handled by the alert aggregator. However, some emergencies, such as the Virginia Tech and Omaha mall shootings, require a highly targeted and local system for the delivery of alerts. These narrowly focused and targeted alerts should not be funneled through the alert aggregator.
Through research and development efforts we recommend to the committee that there be multiple alert aggregators. At a national level there should be several regional aggregators which will primarily serve their region but also provide backup and load balancing facilities.

We also recommend to the Committee that they specifically allow for commercial and non-commercial carriers, such as universities, to have localized alerting systems. And that they allow for such private alerting systems to be connected via standard interfaces to the national alerting gateways to also provide national alerts.

The proposed model seems to be based on a "push" concept, in which authorized alert agency(s) publish their alerts to the Aggregator. We also would like to see a "pull" model, where the Aggregator can subscribe to authorized alerting services (NWS, etc.), so they do not need to change their current processes (as long as they publish in valid CAP).

In addition, it is unclear if any "filtering" is performed on the types of alerts that are broadcast. For example, suppose an agency is authorized to issue AMBER alerts to the Aggregator. What would prevent them from also issuing other types of alerts? We propose that the Aggregator and/or Gateway should have some type of filtering function to ensure that only high-priority alerts (Tornado Warnings, etc.) can be issued. In addition, there should be some "reality checks" performed by the Gateway to ensure, for example, that the alert geographical scope makes sense based on alert type (e.g. a Tornado Warning cannot be sent to an entire state).

13. **FCC Statement**: *We seek comment on the CMSAAC's recommendation that the CMAS use CAP as the basic alerting protocol from the alert initiator to the alert gateway. We also seek comment about the use of CAP as a general, system-wide CMAS interface. Is use of CAP currently practicable in the context of CMAS? If CAP use were mandated, how quickly could such use be introduced by all CMAS participants? We note that we have specifically mandated use of CAP recently in our EAS Second Report and Order, where we concluded that use of CAP would provide specific benefits to the evolving EAS. As noted above, one of the key benefits of CAP is that it ensures that diverse alert systems and technologies can participate within a common, transparent framework. Would CAP as utilized in the context of CMAS promote similar transparency? To the extent that commenters believe that the use of CAP as proposed would not be appropriate, they should discuss in detail any alternative protocols.*

    PTT Response: CAP is an appropriate protocol for alert formatting. The use of CAP as the "alerting protocol" between the alert initiator and the alert gateway has the advantage that CAP is currently in use for the distribution of weather alerts. However, there are several drawbacks to the use of CAP.

    The protocol used for alerting should provide an unambiguous structure for defining an alert. The structure of CAP allows an alert request to be represented validly in multiple ways. This ambiguity in the message structure increases the chance that alert messages will not be processed, or delivered, correctly.

    CAP itself is not a protocol, but rather an XML file format. The use of files to integrate systems and as the basis of a network protocol causes several problems. First as the Committee asks (§III.A.1, No 11), the security and trust model requirements require the creation of a higher layer communications protocol that must be used to deliver the CAP file. Second the transference of files between each system that makes up the alert aggregator and alert gateway increases the costs and timeliness associated with processing a message. Third an entire CAP file must be transferred and processed to determine its validity, acceptability, and if the alert is applicable to the receiving system

    However, our experience based on the NOAA feeds from http://www.weather.gov/alerts/ is that formatting can vary quite a bit while still being compliant to the CAP standard. Based on this, we would be very concerned about the technical recommendations in section 10.3.2 that make assumptions about collapsing the CAP INFO blocks. If these rules were applied to the NOAA CAP today, some undesirable consequences would result. Typically, NOAA documents each alert in a state or the US as an INFO block, and many share the same HEADLINE ("Short Term Forecast", "Urgent – Weather Message", etc.). We do not recommend reformatting the original CAP—it should be up to the creator to ensure it follows OASIS standards.

14. **FCC Statement:** *We seek comment on whether we should adopt a character limit for alerts transmitted over the CMAS. We note that the CMSAAC recommended that, at least initially, the technical limit of any CMAS alert should be 90 characters of text. Commenters should provide detailed technical explanation in support of their positions and explain the relationship between "payload" and "displayable message size" as referenced in the CMSAAC's recommendations?*

    PTT Response: We agree in principle with the 90-character text limit. However, it is difficult to reconcile this requirement with the message content requirements (10.3.2.10). We would like to see some real-world tests and examples of this requirement, because we do not believe it is feasible for the majority of alerts that are issued by NWS.

    In our work in developing a system to send broadcast SMS messages on CDMA networks, we have found that the maximum length for such a message is 120 characters and that the practical limit will be somewhat less.

15. **FCC Statement:** *We also seek comment on whether and to what extent emergency alerts should be classified. We specifically seek comment on the CMSAAC's recommendation that there be three classes of Commercial Mobile Alerts: Presidential-level, Imminent threat to life and property; and Child Abduction Emergency or "AMBER Alert" Service.*

    PTT Response: We agree with the CMSAAC's proposed definition of "Imminent threat to life and property" as defined in the text. We recommend that alerts be minimally classified as imminent danger, warning, and no threat. To require any additional levels of classifications or priorities will conflict with the existing specifications for broadcast SMS messages in the GSM and CDMA systems. There does need to limitations on types of messages sent out in order to avoid "alert" fatigue on the part of the end user. Messages have to be perceived as highly relevant to the user because of both location and severity of the event.

16. **FCC Statement:** *We also seek comment on the content of CMAS alerts, including the CMSAAC's recommendation that all service providers support, at minimum, a capability for a text based common alerting message format support across multiple service platform technologies*

    PTT Response: We agree that text-based messages across multiple platforms should be the minimum capability for all service providers, and text-only for an initial system.

17. **FCC Statement:** *The CMSAAC also recommended that the elements of a Commercial Mobile Alert Message (CMAM) should be (1) event type or category, (2) area affected, (3) recommended action, (4) expiration time with time zone, and (4) sending agency. We seek comment on these choices. Are they consistent with accepted industry practices for emergency alerts? Are they consistent with the evolving concept of CAP-formatted messages? The CMSAAC anticipated that the elements of a CMA would evolve as experience is gained by alert initiators. We seek comment on this assumption. How might CMAM elements evolve over time?*

PTT Response: We do not recommend the use of CMAM. For our reasoning see our prior comments to the Committee's questions. As stated earlier, we are skeptical that the CMAM-required message content can fit within 90-characters. We would prefer to see the *event type* and *area affected* the only required elements. The *expiration time*, *issuer*, *media sources*, and *recommended action* should be optional, if space permits.

18. **FCC Statement**: *The CMSAAC also recommended a method for the automatic generation of alert text by extracting information from CAP fields, SAME codes and free-form text, but proposed that the CMAS allow the generation of free text in Amber Alerts and Presidential alerts.*[35] *. We seek comment on this recommendation. We also seek comment on whether Presidential and Amber alerts can be structured to use automatic text.*

    PTT Response: We agree with the proposal for free text entry for only Presidential Alerts and AMBER Alerts. However, there should be some human approval mechanism on the Alert Gateway before any alerts are issued with free text entry.

    We are curious how the CMSAAC envisions that "ad hoc" alert messages would be issued for scenarios such as Hurricane Katrina or the Virginia Tech shooting, which was mentioned in section 5.3.2, but it is unclear how such an alert could be issued by CMAS. For example, is it coded as a Civil Emergency Notification (CEN)? Would it be assumed that such a message is also broadcast over EAS? Would the issuer be able to enter free-form text to provide specific instructions?

19. **FCC Statement:** *We also seek comment on the CMSAAC's recommended set of standardized alerting messages. Should the alert message include telephone numbers, URLs or other response and contact information in certain Commercial mobile alerts?*[36] *Is there public safety value to the inclusion of such information in a Commercial mobile alert? What, if any, would be the impact on the network? In prior emergencies, mobile traffic increased to the point of network congestion. What would be the impact on network congestion if subscribers were directed to a specific number (such as a "311" number in New York City) or URL?.*

    PTT Response: We take issue with section 5.2.3.1, which states that the message should not contain any URLs. We believe that this decision should be left optional to the CMSP whether to include a URL or not.

    We also take issue Requirement 5.3.1, which specifies that the message should include "Check local media for info". First, this should not be a requirement (it goes without stating), and secondly, it would be more helpful to travelers if the CMSP may optionally add a reference to a specific media. In our project tests we include the capability to associate a cell tower with a specific media station, this will allow CMSP to specifically encode the broadcast from each cell tower with relevant media instructions. A person in receipt of the message driving through the cell tower range can then access that media that is broadcasting additional emergency information.

20. **FCC Statement:** *We seek comment on what level of precision we should require for the geographical targeting (geo-targeting) of CMAS alerts. In section 5.4 of its recommendations, the CMSAAC acknowledged "that it is the goal of the CMAS for CMSPs to be able to deliver geo-targeted alerts to the area specified by the Alert Initiator." However, the CMSAAC recommended that, due to current limited capabilities on the part of CMS providers, "an alert that is specified by a geocode, circle or polygon . . . will be transmitted to an area not larger than the CMSP's approximation of coverage for the county or counties with which that geocode, circle or polygon intersects." We seek comment on this recommendation, including the assertion that technical limitations currently preclude dynamic geo-targeting at a level more granular than the county.*

    PTT Response: We do not agree with some of the assertions in section 5.4 regarding geo-targeting of areas smaller or larger than a county. Geo-targeting at areas lower than a county is clearly possible with cell broadcast. In fact the switching equipment allows broadcast to a specific sector on a single tower. The CMSP should know where their towers are located and can broadcast the message from all towers with range within the specific affected area (county, polygon, or circle).

    Additionally, requirement 5.3.1 recommends using the geocode in priority to the polygon or circle. We recommend the opposite, as the polygon will always be more geo-specific than the county-level geocodes. We believe that the Committee should require a high level of precision for the geographic targeting of alerts. We recognize that most of the alert types that the Committee and the CMSAAC have considered are very large scale events, like severe weather, and that large coverage area, like counties, makes sense in those scenarios. To fulfill the Committee's goals of providing "geo-specific", accurate and reliable information the alerts need to be targeted with a high degree of geographic precision. To illustrate the need for this precision one should consider that a municipality may send an alert for a chemical spill from an overturned tanker, or that first responders may send alerts in response to a shooting event like Virginia Tech. Broadcasting these alerts to an entire county may cause unintended concern or panic, and that may hinder the first responders ability to react by flooding emergency lines with inquiries or false tips. Or worse, people may loose faith in the alerts by receiving too many alerts that do not affect them.

    We have tested the ability to do a broadcast SMS message on a CDMA system that targeted an individual cell or like device with receiving capability. So we are confident that there are no technical hurdles that will prevent CMSP's from providing such geo-targeted alerts

21. **PTT Response**: No comment regarding the recommendations in section 5.4.

22. **PTT Response**: No comment on the requirements for alerts received by people with disabilities and the elderly.

23. **FCC Statement:** *We seek comment on the technical feasibility of providing commercial mobile alerts in languages in addition to English. The CMSAAC suggested that there may be fundamental technical challenges to implementing parallel alerts in languages in addition to English. We seek comment on this view. We recognize the significant public safety interest in delivering alerts to speakers of languages other than English and strongly affirmed this principle in our May 2007 EAS Second Report and Order. CMSAAC also asserted that multilingual (and geo-targeted) alerting would raise latency (alert delay) concerns.[46] How would requirements for multi-language alerts affect the generation and distribution of messages on a local, state and national level?*

    PTT Response: We agree with the CMSAAC decision to defer non-English language support due to the technical challenges.

24. **PTT Response**: No comment regarding procedures for provider participation in the service.
25. **PTT Response**: No comment regarding the point of sale notice.
26. **PTT Response**: No comment regarding how providers communicate participation in the service.
27. **PTT Response**: No comment regarding clear and conspicuous notice.
28. **PTT Response**: No comment regarding disclosure of participation.
29. **PTT Response**: No comment regarding how notice of the service is given.
30. **PTT Response**: No comment regarding the interpretation of the WARN Act timeline.
31. **PTT Response**: No comment regarding the method of maintaining provider election and withdrawal information.
32. **PTT Response**: No comment regarding how providers file for adoption of the CMSAAC guidelines.
33. **PTT Response**: No comment regarding provider withdrawal from the program.
34. **PTT Response**: No comment regarding subscriber withdrawal from the system.

35. **FCC Statement:** *Section 602(b)(2)(E) states that "any commercial mobile service licensee electing to transmit emergency alerts may offer subscribers the capability of preventing the subscriber's device from receiving such alerts, or classes of such alerts, other than an alert issued by the President."[64] The CMSAAC recommended that the CMS providers should offer their subscribers a simple opt-out process.[65] With the exception of presidential messages, which are always transmitted, the CMSAAC recommended that the process should allow the choice to opt out of "all messages," "all severe messages," and AMBER Alerts.[66] The CMSAAC suggested that, because of differences in the way CMS providers and device manufacturers provision their menus and user interfaces, CMS providers and device manufacturers should have flexibility on how to present the opt-out choices to subscribers. We seek comment on the recommendations of the CMSAAC with respect to three choices of message types that a subscriber should be allowed to choose to opt out of receiving. We also seek comment on the CMSAAC recommendation that CMS providers and device manufacturers should have flexibility or whether the Commission*

should establish baseline criteria for informing subscribers of this capability and if any uniform standards for conveying that information to subscribers is required. We understand that current and future devices have different user interfaces and menu structures for enabling and disabling device features. To what extent is a uniform methodology for disabling this feature necessary? Are there more classes of alerts that should be considered?

PTT Response: We are generally not in favor of the "opt-out" requirement in 5.5.3. We feel that the capability of opting-out will defeat the purpose of the program if a large number of potential users opt-out due to concerns about battery usage, etc. If this requirement moves forward, we would prefer that users utilize the SMS filtering features of their device to filter undesired messages rather than making this a universal feature of the program.

36. **FCC Statement:** *Section 602(b)(2)(E) also provides that the Commission shall, within two years of the adoption of the technical requirements, "examine the issue of whether a [CMS provider] should continue to be permitted to offer its subscribers an opt-out capability."[67] We seek comment on the appropriate mechanism for doing so. Further, we seek comment on whether the Commission can expand the scope of this inquiry to other questions concerning the development of the CMAS. We note that the CMSAAC recommended this result because the CMAS is a new and untested system and will need periodic review as it is deployed.[68] We seek comment on this recommendation.*

    PTT Response: We agree that the opt-out capability should be re-considered in the future. We would like to see it done sooner than 2 years. Consumer complaints should be considered, as well as success stories in cases where CMAS has saved lives.

37. **FCC Statement:** *Section 602(b)(2)(C) states "[a] commercial mobile service licensee that elects to transmit emergency alerts may not impose a separate or additional charge for such transmission or capability." Does this provision completely preclude a participating service provider's ability to recover costs associated with the provision of alerts?[70] What about CMAS-related services and technologies that are not used to deliver CMAS? Should the section's reference to "transmission or capability" be read narrowly? For example, much of the alert technology will reside in the subscriber's mobile device. Can the CMS providers recover CMAS-related developmental costs from the subscriber through mobile device charges based on a determination that mobile devices lie outside the "transmission or capability" language of the section?*

    PTT Response: We would also like to clarify whether the "no charge" provision applies to additional services that the provider may make available to the user for additional information, multimedia data, etc. After the initial transmission the CMSP should have the option to provide additional information through data channels as requested by receivers of the alert, where normal data rates would apply. This should be at the discretion of the CMSP.

38. **PTT Response**: No comment regarding DEAS implementation.

39. **PTT Response**: No comment regarding DTV interface.

40. **FCC Statement:** *Section 602(f) of the WARN Act provides that the Commission shall "require by regulation technical testing for commercial mobile service providers that elect to transmit emergency alerts and for the devices and equipment used by such providers for transmitting such alerts." We seek comment on what type of testing regime the Commission should require. We note that the CMSAAC proposed that in order to assure the reliability and performance of this new system, certain procedures for logging CMAS alerts at the Alert Gateway and for testing the system at the Alert Gateway and on and end-to-end basis should be implemented.*[72] *We seek comment on these proposed procedures. Do they satisfy the requirements of section 602(f) of the WARN Act? We particularly seek comment on whether there should be some form of testing of the CMAS that sends test messages to the mobile device and the subscriber.*[73] *Do the EAS testing rules offer a model for such tests? In those rules, internal systems test are combined with tests that are heard (or in some cases seen) by the public. Should some similar form of test that alerts the public be required in the CMAS? Should the testing process be invisible to the subscriber or should all subscribers participate in certain tests? If testing involves subscribers, how should subscribers be made aware of such tests?*

    PTT Response: We agree that periodic end-to-end technical testing is desirable. We would like to see something similar to EAS, where monthly tests are required. Citizens have become accustomed to these tests, and we see no issues with all users receiving a "REQUIRED MONTHLY TEST" message occasionally to verify that their device is correctly configured.

41. **FCC Statement:** *As noted earlier, the Commission originally intended to consider in its rulemaking in EB Docket No. 04-296 whether wireless mobile service providers should be included in the EAS. Notwithstanding various operational differences between the EAS and those requirements mandated by the WARN Act (chiefly, the voluntary participation model of the latter), both alert systems will provide important emergency information to American citizens. As such, both systems would seem to qualify for inclusion in the "national alert system," to be developed and coordinated by FEMA, as envisaged by President Bush's June 2006 Executive Order.*[75] *We seek comment about how the CMSAAC's proposals for a CMAS relate to the directives contained in that Executive Order. We also seek comment about the overall compatibility of the CMAS with the EAS (i.e., in addition to the specific questions that have been raised earlier in this NPRM). Should we mandate such compatibility? What steps would we need to take to ensure such compatibility? As related above, the CMSAAC has proposed use of CAP1.1 as the standard CMAS alert interface, and the Commission has mandated that CAP1.1 shall also be the standard interface for the evolving EAS (if it is adopted by FEMA). Would adoption and incorporation of CAP1.1 per the CMAS in and of itself ensure that it's compatible with a CAP-formatted EAS alert delivery system? If not, what modifications to the CMSAAC's proposals would be necessary to ensure such compatibility with the future National Alert System required under EO 13407? Finally, we also seek comment on what additional statutory authority, independent of the WARN Act, we have to implement a mobile alerting system.*

    PTT Response: Moving EAS to a CAP-based format would be a significant and positive step towards compatibility between EAS and CMAS and is probably most effectively accomplished through a mandate by the FCC.

The FCC document had an opened-ended request for "Any alternatives to the CMSAAC's Recommendations." Below are the PTT recommendations that we should be submitted to the FCC

The use of CAP and CMAC

The CMSAAC recommends to the Commission that CAP and CMAC be used as a protocol between systems that form the CMAS. The Committee poses specific questions on this topic in sections III.A.1, No 11 and III.A.3, No 14 and to which we provide specific answers. Both CAP and CMAC are not computer protocols but are XML file formats. As such, noted in our response to §III.A.1, the trust model and other requirements require that a higher layer protocol be implemented. Our recommendation is that Committee require a protocol that follows industry standard practices, and will fill the requirements of the trust model and the delivery of the alert message and other data. This type of protocol definition and practice has created many long lived, flexible, and robust systems such as email and http. We further recommend to the committee that this protocol, once developed, be submitted to the Internet Engineering Task Force (IETF) as a Request For Comment (RFC) for inclusion as a networking standard.

Rebroadcast of alerts

The CMSAAC stated that the CMSP rebroadcast alert until such time as the alert has expired. The cellular telephone equipment that is currently in the market, and current industry specifications, will not filter out duplicate messages. The switching equipment has cell broadcast transmission rate limits. As the system becomes more geo-specific (e.g. a messages directed to individual towers) the switch could easily be overloaded with multiple retransmissions to specific towers. Furthermore constant re-broadcasting will create receiver fatigue. We recommend to the Committee that instead the alerts be periodically rebroadcast and that the rebroadcast be done by the alert aggregator according to the nature and severity of the alert.

Targeted delivery of alerts to the CMSP

The CMSAAC stated that the alert aggregator send alerts to the CMSP on a state level. The committee should consider a small tier three rural provider that has coverage for example in several counties in Nebraska, Iowa, and Missouri. Such a provider may receive redundant events for each state as well as any alert generated by each state or by municipalities. The task of filtering out duplicate and inapplicable messages then falls on each and every CMSP, regardless of their size and technical sophistication. To ensure the accuracy of the alerts broadcast, we recommend that the Committee require that alerts be send to the CMSP only when that alert impacts the geographic area covered by the CMSP, hence the alert aggregator should do some geographic filtering of the alert "push" to the CMSP's.

About Purple Tree Technologies and Electronic Data Systems

PTT and EDS have been business partners since 2004, jointly developing a the next generation emergency alert solution. PTT is a technology company in Columbia, Missouri focused on creating emergency alert technology. EDS is a global technology services corporation delivering innovative, secure technology solutions for clients throughout the world.